UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,156	07/14/2003	Seth Jerome Robertson	61164-0003	9506

9629 7590 02/16/2007

MORGAN LEWIS & BOCKIUS LLP
1111 PENNSYLVANIA AVENUE NW
WASHINGTON, DC 20004

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
31 DAYS	02/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/620,156	ROBERTSON ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 1 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 July 2003*.

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *1-18* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-2, drawn to classifying event messages with labels, combining labeled alerts and aggregating combined alerts to produce a notification, classified in class 713, subclass 153.

II. Claims 3-12, drawn to receiving a plurality of event messages and processing the messages by clustering packets, classified in class 726, subclass 11.

III. Claims 13 & 16, drawn to combining alerts from an intrusion detection system with alerts from an anomaly detection system and prioritizing a combined alert, classified in class 726, subclass 23.

IV. Claims 14-15, drawn to storing outputs from sensors and storing an using a plurality of production models for an initial event evaluator and alert filtering modules, classified in class 726, subclass 26.

V. Claim 17, drawn to displaying threat information to a user, classified in class 715, subclass 736.

VI. Claim 18, drawn to detecting network connections that are likely surveillance probes originating from malicious sources, classified in class 726, subclass 22.

The inventions are distinct, each from the other because of the following reasons:

2. Inventions I-VI are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct if they do not overlap in scope and are not

obvious variants, and if it is shown that at least one subcombination is separately usable. In the instant case, **subcombination I** has separate utility such as managing a hierarchy of alerts, not requiring clustering packets (II), multiple detection systems (III), multiple production models (IV), displaying threat information (V) or detecting probes (VI); **subcombination II** has separate utility such as packet classification for faster processing, not requiring classifying event messages with labels and then combining labeled alerts, multiple detection systems, a plurality of production models, displaying threat information or detecting surveillance; **subcombination III** has separate utility such as internal and external security, not requiring classifying event messages with labels and then combining labeled alerts, clustering packets, multiple production models, displaying threat information or detecting probes; **subcombination IV** has separate utility such as customer-specific profile alerting, not requiring classifying event messages with labels and then combining labeled alerts, clustering packets, multiple detection systems, displaying threat information or detecting probes and **subcombination V** has separate utility such as a graphical interface to display monitoring status, not requiring classifying event messages with labels and then combining labeled alerts, clustering packets, multiple detection systems, multiple production models or detecting probes. See MPEP § 806.05(d).

Because these inventions are independent or distinct for the reasons given above and there would be a serious burden on the examiner if restriction is not required because the inventions require a different field of search (see MPEP § 808.02), restriction for examination purposes as indicated is proper.

3. The examiner has required restriction between subcombinations usable together. Where applicant elects a subcombination and claims thereto are subsequently found allowable, any

claim(s) depending from or otherwise requiring all the limitations of the allowable subcombination will be examined for patentability in accordance with 37 CFR 1.104. See MPEP § 821.04(a). Applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS

KAMBIZ ZAND
PRIMARY EXAMINER

February 12, 2007